Seguridad Informática en el Siglo xxi: Una Perspectiva Jurídica Tecnológica Enfocada Hacia las Organizaciones Nacionales y Mundiales

Computer Security in the Twenty-First Century: on national and world organizations a technology to legal perspective

[1]Juan José Candelario Samper, [2]Moisés Rodríguez Bolaño

Universidad Nacional Abierta y a Distancia - UNAD,
Escuela de Ciencias Básicas Tecnología e Ingeniería, Santa Marta, Colombia.

[1]juan.candelario@unad.edu.co [2]moises.rodriguez@unad.edu.co

Recibido: 18/04/2014 • Aprobado: 22/06/2014

Resumen

Sin ninguna duda, el indetenible progreso de la informática en pleno siglo XXI ha facilitado que la información se transforme en un insumo comercial para una gran cantidad de naciones alrededor del mundo y en un activo de gran valor que, bajo cualquier circunstancia, debe ser protegido para garantizar los elementos básicos de la seguridad: integridad, confidencialidad y disponibilidad. Las medidas convenientes para conseguir este objetivo pueden discriminarse desde muchos ámbitos o aspectos: administrativo, organizativo, físico, técnico, legal, pedagógico y jurídico. En este artículo se pretende dar a conocer algunos parámetros que se han estipulado internacionalmente con relación a la seguridad informática, específicamente en lo que tiene que ver con la protección de datos de los usuarios en organizaciones, con un determinado propósito. A partir de lo anterior, lo que se intenta es crear un tipo de cultura con respecto a fortalecerse en esta era de la información, e indagar por la existencia de políticas de seguridad de la información ajustadas tanto a la legislación nacional como internacional, alineadas en lo fundamentado en los distintos estándares que se han formulado para alcanzar tales fines. Existen mecanismos como la detección y defensa contra virus e intrusiones o para conseguir confidencialidad basados en cifrado simple que se emplea para visualizar la perspectiva que en materia jurídica y legal se ha expandido por todo el globo terráqueo; este radica en los contenidos que proponen los decretos, leyes y enmiendas estipulados como mecanismos de regulación en asuntos relacionados con dicha contextualización.

Palabras Clave: *derecho internacional, marco legal y jurídico, ciencia y tecnología, ataques y delitos informáticos, tecnología.*

Abstract

Without any doubt, the unstoppable progress of computer technology in the XXI century has been a significant facility for which information is transformed into a commercial input for a lot of nations around the world; an outstanding asset value, which under all circumstances must be protected to ensure the basic elements of security: integrity, confidentiality and availability. Appropriate measures to achieve this goal can be discriminated from many areas or aspects: administrative, organizational, physical, technical, legal, educational and legal. This article plans to publicize the existence of certain peculiarities that have provided internationally with regard to security matters related specifically to protect user data in organizations with a particular purpose. From the above, which is also intended to create a kind of culture with respect to the position it is necessary to strengthen the "information age", with the firm intention to investigate the existence of security policies of the adjusted data at both national and international legislation, aligned in based on the different standards that have been developed to carry such purposes. There are mechanisms such as detection and defense against viruses and intrusions or for confidentiality based on simple encryption that is used to display the perspective that legal and legal matters has expanded across the globe, lies in the content proposed by the decrees, laws and amendments stipulated as a mechanism regulating its affairs of such contextualization.

Keywords: *international law, legal framework and legal, science and technology, cybercrime attacks and technology.*

I. Introducción

El impacto de las Tecnologías de la Información y las Comunicaciones (TIC) no es ajeno al Derecho; por el contrario, cada día, los avances de la tecnología imponen mayores retos a los operadores jurídicos, a los cuales hay que responder desde la legislación nacional, la legislación internacional, el derecho comparado, la autonomía de la voluntad privada, las mejores prácticas existentes en la industria y las normas que permitan dar un tratamiento uniforme a problemáticas que experimentan las organizaciones, cualquiera que sea la latitud en que estén ubicadas [1].

Como bien se sabe, actualmente, hay un sinnúmero de problemas que acontecen en internet, entre otros, acciones que tornan vulnerable la información tanto personal como organizacional, teniendo en cuenta que las Tecnologías de la Información y la Comunicación son el instrumento primordial de funcionamiento en los distintos niveles de la sociedad; esto es directamente proporcional a un tipo de subordinación informática, en cualquier tipo de sector que se utilicen (industrial, comercial, educativa y cultural) donde a simple vista es posible apreciar su profundo impacto en cada elemento que conforma la sociedad.

La información, como un elemento más al interior de una organización, se considera un activo valioso, ya que de ahí se toman decisiones importantes para el desarrollo de los objetivos corporativos y, a su vez, se le brindan al usuario elementos de juicio para su permanencia como cliente; de ahí, la necesidad de ser protegida. Es así, como, por ejemplo, en materia legislativa, Colombia se ha unido con otras naciones en cuanto a la normatividad que protege los activos informáticos. Para tal fin, se cuenta con la Ley

1273 de 2009, la cual regula y penaliza el delito informático, como suplantación, fuga de información, etc., o también la Ley 527 de 1999. No obstante, la inseguridad y desconfianza, no solo de las directivas organizacionales, sino también de los diversos estamentos de la sociedad, en calidad de usuarios, consumidores y titulares de datos personales, aún prevalecen.

II. Antecedentes.

No cabe la menor duda de que el concepto de seguridad es un término asociado a la confianza, certidumbre o contingencia. Si n embargo, a pesar de que dicho concepto emite un sentimiento protector hacia lo que respecta salvaguardar, es importante que se aclare que el componente de peligro, es un elemento que está en constante acecho esperando la oportunidad para provocar algún tipo de dificultad que involucre la estabilidad de la organización, independientemente de las regulaciones propias que se tomen en un entorno, que se considere seguro.

En Colombia, así como en los demás países del mundo, el valor de la información, como consecuencia de un proceso especializado e intelectual en un área en particular, requiere de mecanismos aptos que busquen y garanticen su adecuado y óptimo funcionamiento, a fin de protegerla y asegurar su estabilidad. Es así, como una de las mayores preocupaciones del hombre, a lo largo de la historia de la humanidad, ha sido siempre la seguridad; su anhelo constante de mantener protegida y conservada la información de una forma segura. Por tanto, desde tiempos ancestrales, se han establecido múltiples formas y métodos para conseguir dicho propósito.

Los canales de comunicación han venido evolucionando. En un principio eran informales, tanto en su estructura como en su utilización. Hoy en día, el uso masivo de la informática, pasó de un sistema de procesamiento electrónico de datos, a un sistema de información basado en computadoras, el cual tomó auge como sistema de información gerencial.

En la medida en que la tecnología avanza exponencialmente, las amenazas, peligros e inseguridades a los que se encuentra sujeta la información procesada y almacenada, es mucho mayor. En efecto, la información, que comprende un valor incalculable en materia organizacional y, sin duda alguna, una significativa y apetecida ventaja de naturaleza estratégica en el mercado donde se desenvuelve, se torna en algo extraordinariamente llamativo competitivamente. Por lo tanto, la protección de la información se convierte en algo vital para una organización y de gran impacto en la cultura organizacional.

A. Seguridad informática.

Se define contextualmente como un conjunto de conocimientos sistemáticos orientados a conseguir niveles altos de seguridad en materia de sistemas informáticos. Ahora bien, durante los últimos años, se ha venido implementando en el país y en muchos países en todo el mundo, una serie de normatividades y elementos legislativos (leyes) que buscan penalizar y judicializar aquellas personas que se vean envueltas en acciones reprochables, con el único objetivo de sacar una ganancia de la misma [2].

El objetivo principal, entonces, de la seguridad informática es proteger y salvaguardar la información desde su confidencialidad, integridad y disponibilidad a fin de evitar problemas en materia de autentificación; es decir, el impedimento de acciones suplantadoras, y que realmente se brinde una garantía en cuanto a que quien remite el contenido de un mensaje es realmente el titular de la cuenta de buzón.

Fig. 1 *Seguridad Informática [2]*

B. Comportamientos inadecuados atentatorios de la seguridad informática: el delito informático.

De una forma genérica, flexible y bajo una terminología lo más sutil y pragmática posible, el delito informático se conceptualiza como todo acto, comportamiento y/o conducta indebida, ilícita e ilegal que propicie ser razonado como criminal, orientado a la alteración y/o destrucción de cualquier sistema de información o alguno de sus componentes que la integren, generando como producto final un daño lesivo al tratamiento de la información, y dejando bajo amenaza a las organizaciones sin tener un servicio jurídico que la respalde [3].

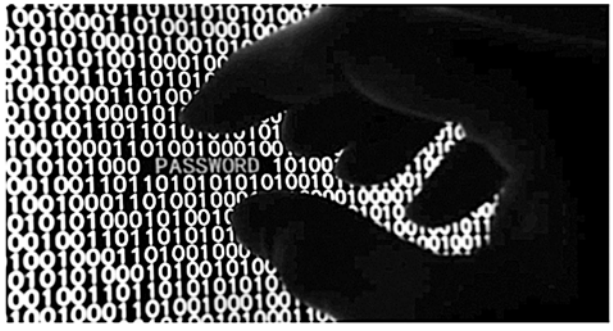

Fig. 2 *Delito informático. [3]*

Ahora bien, no sería nada extraño, en pleno siglo XXI, que las máquinas computacionales se usen para distintas formas y maneras de crímenes, dentro de las que es posible resaltar el fraude, robo, espionaje, sabotaje y hasta asesinato; es decir, se ha dado pie a esta clase de criminalidad que se encuentra entrañablemente mancomunada al desarrollo tecnológico e informático. En Colombia, así como en muchos países del mundo, el delito informático se ha vuelto el pan de cada día**.** En los diferentes medios de comunicación, hablados o escritos, se encuentran noticias de distintos tipos de abusos relacionados con la tecnología. Por ejemplo, el 6 de mayo del año 2014, salió a la luz pública uno de los mayores escándalos en política que se haya registrado en el país: las chuzadas y espionaje ilegal que se le presume al candidato a la presidencia por el partido Centro Democrático, Óscar Iván Zuluaga, ejecutado por ingenieros expertos en lo referente a ataques y defensas de un sistema de información [4].

Fig. 3 *Criminalidad Informática [4].*

La justificación y los detalles que particularizan la criminalidad informática radica esencialmente en su carácter tecnológico y de la información; es decir, la especificidad, que se le atribuye a la máquina computacional en conjunto con sus tareas más importantes como son: el procesamiento y transmisión automatizados de datos y el diseño, adecuación y/o utilización de software para tales fines.

Cualquier comportamiento y/o conducta que no maniobre sobre la base de estas, aunque pueda que resulte implicada en un evento delictivo (o estimable de sanción penal en su caso determinado), no tendrá ya la especificidad (tal y como ocurre con la mayoría de ataques orientados a la parte física –hardware–) y por ende correspondería ser retirada del estudio de la delincuencia sujetada a la informática o tecnologías de la información (TIC).

C) Sujetos del delito informático.

Desde el punto de vista de la ciencia del derecho, más en particular de la penal, un comportamiento indigno presume la existencia de dos sujetos: un sujeto activo (el que realiza la acción) y otro pasivo (el que recibe la acción), quienes, al mismo tiempo, pueden ser una o varias personas de tipo natural o jurídica. Por lo tanto, el bien jurídico protegido será definitivamente, el elemento determinador de los sujetos y de su posición con respecto al delito ejecutado.

1) ***Sujeto activo.*** Se entiende por tal, a la persona que ejecuta toda o una parte de la acción descrita por el tipo penal. De hecho, las personas que ejecutan los delitos informáticos son aquellas que tienen particularidades que no presentan el común denominador de los bandidos; en otras palabras, los sujetos activos tienen competencias y cualificaciones para el uso y manejo de los sistemas informáticos y, habitualmente, por el entorno donde trabajan, se ubican en sitios de alto grado de importancia, en los cuales se manipula y administra información sensible; o bien, son ingeniosos en la rutina de los sistemas informatizados, aun cuando en muchos de los casos no desarrollen un ejercicio de actividades laborales que conlleven a este tipo de acciones poco éticas [5].

Fig. 4 *Sujeto activo del delito informático [5]*

2) Sujeto pasivo. Es la persona titular y/o propietario del bien jurídico (información y demás elementos informáticos) que la ley protege (en calidad de víctima) y quien recibe la actividad típica del sujeto activo. Dentro de este contexto situacional, se debe diferenciar el sujeto pasivo o víctima del delito, que es sobre quien reincide (o recibe) el comportamiento de acción u omisión que ejecuta el sujeto activo; en el caso más concreto de un delito informático, es posible que las víctimas sean individuos (persona natural o jurídica), bancos, compañías de financiamiento, gobiernos, etc., que usan sistemas automatizados y configurados de información, corrientemente enlazados a otros. Cabe resaltar que el sujeto pasivo del delito para un proceso investigativo, es fuertemente significativo para tal fin, ya que a través de este es posible tener conocimiento de los diferentes actos indebidos que perpetran los delincuentes informáticos, con el propósito de prever las acciones y estrategias que mitiguen o neutralicen los efectos negativos que los ataques del *modus operandi* de los sujetos activos propicien en el sistema de información [6].

Fig. 5 *Sujeto pasivo del delito informático [6*]

III. Tipos de Delitos Informáticos.

De la misma forma que ha venido avanzando la tecnología, se han incrementado los delitos informáticos; la diversidad de las conductas comportamentales integrantes de esta clase de acciones indebidas e ilícitas no tiene un punto fijo de imaginación y apropiación [7].

Fig. 6 *Tipos de delitos informáticos [7]*

Dentro de este contexto, es posible resaltar el ingenio de muchas personas, que se han valido de su profesión en el área de sistemas, tecnología y telecomunicaciones, para arrinconar a las empresas pues se aprovechan de sus competencias, talento y recursos para transgredir la seguridad de sus sistemas de información y hacer con lo que sustraen un verdadero festín.

Algunas investigaciones llevadas a cabo en países como Alemania, México y Estados Unidos, exponen que el posible límite de una persona con el conocimiento para ejecutar un delito informático va articulado a tres factores o elementos: la imaginación del sujeto quien lo desarrolla, su capacidad técnica y las deficiencias de control que se den en las instalaciones informáticas. Es así, como en la medida que la tecnología evoluciona, se deben tomar las acciones necesarias que contrarresten tales fenómenos.

En la tabla 1, se presentan las clases de conductas delictivas a las que se ven expuestas empresas tanto nacionales como internacionales:

TABLA I.

CATEGORIZACIÓN DE LOS DELITOS INFORMÁTICOS [8]

Grupo de conducta delictiva	Características generales
Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos	Se incluye el acceso ilícito a sistemas informáticos; la interceptación ilícita de datos informáticos; la interferencia en el sistema mediante la introducción, transmisión, provocación de daños, borrado, alteración o supresión de estos; y el abuso de dispositivos que facilitan la ejecución de delitos.
Fraudes informáticos	Incluye la falsificación informática que produzca la alteración, borrado o supresión de datos informáticos que ocasionen datos no auténticos.
Delitos relacionados con el contenido	Este grupo aborda los delitos relacionados con la pornografía infantil.
Delitos relacionados con infracciones de la propiedad intelectual y derechos afines	En orden del cumplimiento del Convenio sobre la Ciberdelincuencia, los países firmantes deben considerar la tipificación de estas conductas como delitos, en su derecho interno.
Delitos relacionados con el robo de servicios	Este grupo comprende las acciones indebidas relacionadas con el hurto del tiempo del computador; la apropiación de informaciones residuales (*scavenging*); el parasitismo informático (*piggybacking*) y la suplantación de personalidad (*impersonation*).
Delitos relacionados con el espionaje informático y el robo o hurto de software	Relaciona lo comprendido con respecto a fuga de datos (data leakage) y la reproducción no autorizada de programas informáticos de protección legal.

IV. Contexto Situacional Jurídico, Legal y Normativo que Penaliza el Delito Informático.

La seguridad informática ha ganado un importante y trascendental valor en el modelo esquemático de implantación e implementación de instrumentos de tipo tecnológicos, tanto físicos como lógicos, que minimicen y/o contrarresten el ingreso no autorizado de invitados no deseados y, por ende, los ataques a los sistemas de información. Dichos instrumentos están enfocados hacia estándares de gestión de la seguridad de la información en los que sobresalen lo dinámico, lo constante sobre lo temporal y lo ocasional.

En efecto, para alcanzar el objetivo trazado sobre un nivel de seguridad adecuado, es indispensable la articulación de áreas del saber que produzcan un significativo impacto en la culminación de dicha acción; vale resaltar que un sistema de gestión no es un factor que garantice totalmente la extinción de los delitos informáticos. Se requiere, además, de un instrumento en materia tecnológica y de la aplicación de acciones de tipo legal y jurídica, como medidas adicionales oportunas. En muchos países del mundo se han propuesto distintos tipos de leyes y normas que regulan las acciones indebidas y las penaliza según lo cometido [8], (Ver tablas 2, 3, 4 y 5).

TABLA II.

Legislación Vigente Para Delitos Informáticos en Latinoamérica [9]

País	Legislación	Características Generales
Argentina	Código Penal, Ley 26388 (2008), Ley 25326 (2000)	Incorporado y realizado una serie de modificaciones al Código Penal argentino, la misma no regula este tipo de delitos en un cuerpo normativo separado del Código Penal (CP) con figuras propias o independientes.
Bolivia	Código Penal, Ley 1768 (1997), Ley 3325 (2006)	Allí incorpora como Capítulo XI, del Título XII, del Libro Segundo del Código Penal, el de "Delitos informáticos".
Brasil	Ley 12737 (2012), Ley 11829 (2008)	Dispone la tipificación criminal de los delitos informáticos y otras providencias.
Chile	Ley 19223 (1993), Ley 20009 (2005), Ley 18168 (2002)	Ley "Relativa a Delitos Informáticos" que de acuerdo con su propio título, regula cuatro artículos, desde los cuales se tipifican varios delitos informáticos.
Colombia	Ley 1273 (2009), Ley 1366 (2009)	Modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "De la protección de la información y de los datos". Se afirma que dicha normativa busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.
Costa Rica	Ley 9048 (2012)	Es una modificación importante del Código Penal de este país. En la misma, agrega una importante cantidad de delitos informáticos al Código Penal, desde los más tradicionales hasta algunos más modernos como la suplantación de identidad o el espionaje cibernético.
Ecuador	Ley Nº 67/2002 (2002)	Regula el comercio electrónico, firmas y mensajes de datos.
México	Reforma 75 del Código Penal Federal (1999)	Mediante reformas del Código Penal Federal, se tipifican los delitos informáticos clásicos teniendo en consideración la fecha de su incorporación.

Fuente: [9]

TABLA III.

Legislación Vigente Para Delitos Informáticos en Norteamérica [8]

País	Legislación	Características generales
Canadá	Código Penal de Canadá (CPC).	Contempla los delitos informáticos puros y los delitos afines como uso no autorizado de la computadora; uso, posesión o tráfico de contraseñas de computadoras; posesión de un dispositivo para obtener servicios informáticos; daños de datos.
Estados Unidos	Adopción en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986.	Constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen.

TABLA IV.

Legislación Vigente Para Delitos Informáticos en Europa [8]

País	Legislación	Características Generales
Alemania	Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986.	Contemplan los delitos como espionaje de datos, estafa informática, alteración de datos, etc.
Austria	Ley de reforma del Código Penal de 22 de diciembre de 1987.	Contempla delitos tales como destrucción de datos, estafa informática. Además, vislumbra sanciones para quienes cometen este hecho utilizando su profesión.
España	Código Penal de 1995 aprobado por Ley Orgánica 10/1995, de 23 de noviembre y publicado en el BOE número 281, de 24 de noviembre de 1995.	Incorpora los tipos delictivos clásicos de la realidad informática de manera global, no limitándose a regular solo los delitos informáticos de mayor conocimiento en la doctrina y otras legislaciones. Es uno de los países de la Comunidad Europea que muestra preocupación por insertar en su infraestructura jurídica los temas de seguridad informática.
Francia	Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.	Aborda la penalización en materia de acceso fraudulento a un sistema de elaboración de datos, sabotaje informático, destrucción de datos, falsificación de documentos informatizados, uso de documentos informatizados falsos.

TABLA V.

Convenios Internacionales Vigentes Para Combatir el Delito Informático [8]

Convenio y/o Tratado	Características generales
Convenio de Cibercriminalidad de la Unión Europea	Firmado el 21 de noviembre de 2001 en Budapest, fue impulsado por el Consejo de Europa y otros países como Estados Unidos y Japón. Consta de varios puntos, entre ellos, definiciones de términos que son necesarios para comprender el espíritu del convenio, (artículo primero), incluyendo los conceptos de sistema, datos de tráfico o proveedor de servicios.
Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional	Entra en vigencia en septiembre de 2003; es el principal instrumento internacional en la lucha contra la delincuencia organizada. La Convención tiene 147 Estados Signatarios y 100 Estados Parte y de la cual el Ecuador es parte; en dicha convención se ponen de manifiesto las reglas básicas sobre la prosecución de Delincuencia Organizada Transnacional. Dichas reglas hacen especial mención de los delitos relacionados con la legitimación de activos y los de corrupción.
Declaración de Principios de la Cumbre de la Sociedad de la Información	Realizada en Ginebra en el año 2005, su objetivo es fomentar la confianza y seguridad en la utilización de las Tecnologías de la Información.

V. Consideraciones Adicionales.

El cada vez más acelerado desarrollo de la tecnología, ligado a la expansión sistemática de la amplia telaraña mundial en distintos aspectos donde interactúa el hombre (social, comercial, cultural y económico) conlleva a un significativo y contencioso aumento proporcional de los desafíos jurídicos y legales en materia de seguridad informática y de la información que regulen la masificación de estos, su uso y abuso, brindando de esa forma, un ambiente y espacio digital mucho más seguro y confiable. Los entes legisladores de cada país del mundo han tramitado a su debido momento diferentes tipos de herramientas estratégicas con el fin de resguardar la información, e impedir que personas inescrupulosas cometan acciones indebidas con datos no autorizados y netamente internos de la empresa u organización.

VI. Aspectos Legales y Jurídicos

Cada una de las leyes, normas, decretos y demás insumos emitidos por entes legisladores y jurídicos, consagra un significativo conjunto de situaciones que procuran determinar un proceso de seguridad lo más completo posible, indicando tajantemente que no todos estos son jurídicamente impactados. Tanto en el ámbito nacional como internacional, los instrumentos propios de la parte legal y jurídica, comprenden la penalización de acciones tales como:

- Acceso ilícito a un sistema de información y/o informático.
- Interceptación ilícita.
- Atentado contra la integridad de los datos.
- Atentado contra la integridad del sistema.
- Abuso de los dispositivos.
- Falsedad informática.
- Fraude o estafa informática.
- Pornografía infantil.

VII. Conclusiones

Si bien es cierto que las organizaciones han invertido una gran cantidad de recursos económicos y humanos en reforzar de forma amplia y masiva la seguridad de los sistemas de información, también es totalmente cierto que los cibercriminales están iniciando la aplicación de tradicionales metodologías

de ataques, que en muchos sistemas informáticos burlan las barreras protectoras implementadas y generan consecuencias poco deseadas por una empresa. El incremento de la astucia y de la complejidad de los ataques está fomentando que se apliquen novedosas técnicas de protección que amparen adecuadamente los activos que aloja un determinado dispositivo de almacenamiento conectado a una red.

La información, como un elemento más al interior de una organización, es considerada no solo un activo inapreciable, sino del mismo modo un singular, pero indudable aliado indispensable para las mismas. De aquí, parte la necesidad de ser protegida, para lo cual se emplean muchos métodos, entre otros, los recursos legislativos. Colombia se equipara con otras naciones en cuanto a la normatividad que protege los activos informáticos, tal como la Ley 1273 de 2009, recientemente promulgada, mediante la cual se regula y penaliza el delito informático como suplantación, fuga de información, etc., o también la Ley 527 de 1999.

Es claro que en la sociedad de la información que caracteriza al siglo XXI, todas las organizaciones, indistintamente sean de naturaleza pública o privada, nacional o multinacional, del sector económico en que ejecuten su razón social y misional, se encuentran ampliamente vinculadas con la tecnología informática (ya sea que adquieran o produzcan activos de información), lo que propicia que la seguridad sea un factor que esté presente de forma permanente.

Tanto la informática, como las Tecnologías de la Información y las Comunicaciones (TIC) requieren de los entes legisladores y jurídicos, y de una evolución constante en materia de ampliación de la tipificación de acciones indebidas que se desarrollan al interior de la amplia telaraña mundial. Si bien es cierto que mundialmente se han realizadograndes esfuerzos por mantener normas y políticas que minimicen los riesgos que estas conllevan y ofrecer un nivel de seguridad hacia los distintos activos de información de una organización, también es cierto que se debe fortalecer esa relación entre la informática y la legislación regulatoria de la misma, a fin de proporcionar un constante apoyo a la sociedad en cuanto a la solución de dichas problemáticas; es decir, un enfoque permanente desde el ámbito legislativo y jurídico de los riesgos, amenazas y vulnerabilidades, como alternativa para proteger las medidas y controles aplicados tecnológicamente.

Referencias

[1] El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27001. [Online]. Disponible en: http://ciruelo.uninorte.edu.co/pdf/derecho/29/12_El%20derecho%20informatico.pdf

[2] Seguridad Informática. [Online]. Disponible en: http://www.proteccionononline.com/mitos-sobre-seguridad-informatica-que-debemos-conocer/

[3] Delito informático. [Online]. Disponible en: http://noticiasdeesquel.wordpress.com/2013/04/29/recomendaciones-para-no-ser-victimas-de-los-delitos-informaticos/

[4] Criminalidad Informática. [Online]. Disponible en: http://www.lavozdelsandinismo.com/nicaragua/2014-05-09/policia-preparada-para-enfrentar-criminalidad-informatica/

[5] Sujeto activo del delito informático. [Online]. Disponible en: http://profesionalespanama.net/curiosidades/top-10-de-condenados-por-delitos-informaticos/

[6] Sujeto pasivo del delito informático. [Online]. Disponible en: http://delixpinfo.blogspot.com/2012/05/tipos-de-delitos-informaticos.html

[7] Tipos de Delitos Informáticos. [Online]. disponible en: http://www.oas.org/cyber/presentations/Tech%20Crime%20-%20Spanish.pdf

[8] Delitos Informáticos: Generalidades. [Online]. disponible en: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

[9] Legislación vigente para delitos informáticos en Latinoamérica. [Online], disponible en: Fuente:http://conaiisi.frc.utn.edu.ar/PDFsParaPublicar/1/schedConfs/2/82-553-1-DR.pdf